Product Support Notice

PSN #	PSN005968u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 15-Dec-21. This is issue #04, published date: 19-Jan-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005968u – CRM Connector R2.x Log4j vulnerabilities.

Products affected

Workspaces for Salesforce (formally CRM Connector R2.x).

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security - **Apache Log4j Vulnerability - Impact for Avaya products*** on support.avaya.com for updates.

CRM Connector 2.2 and 2.1 integrated with AACC are impacted by the Log4j2 vulnerabilities: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105.

The customers that are using CRM Connector 2.x with Elite or POM integration and CRM Connector 2.2 for Oceana are not affected.

The internal analysis has determined that this product is not vulnerable to the related Log4j1x plus JMSAppender vulnerability CVE-2021-4104 and it is also not vulnerable to the related Log4j2 JDBC Appender vulnerability CVE-2021-44832.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.

Resolution

Our recommendation for clients that are using CRM Connector 2.2 and 2.1 integrated with AACC is to upgrade to 2.2.7.4 version and apply the hotfix patch for the aacc3pcc image.

Please note that all the customers that have hotfixes should contact the project team before starting the upgrade to ensure that their hotfixes are ported.

Workaround or alternative remediation

No workaround is available.

Remarks

Issue 4 – January 19, 2022: Include CVE-2021-44832, CVE-2021-4104 vulnerabilities

Issue 3 – December 27, 2021: Include CRM Connector 2.1

Issue 2 – December 21, 2021: PLDS download ID and installation instructions for the hotfix that covers CVE-2021-44228), (CVE-2021-45046), and (CVE-2021-45105)

Issue 1 – December 15, 2021: Initial publication.

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

Always

Download

PLDS ACRM0000073

Patch install instructions	Service-interrupting?
Please see the document “Installing and Configuring Avaya CRM Connector 2.2 for AACC” chapter “Updating Docker images on an existing OVA”. The document can be downloaded from: https://download.avaya.com/css/public/documents/101077223	Yes

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104

Reference https://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

As noted in this PSN.

If you require further information or assistance, please contact your Authorized Service Provider or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.